

84N 10/092,822

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	A. Kent Sievers et al.	Examiner:	David Cervetti
Serial No.:	10/092,822	Group Art Unit:	2136
Filed:	March 6, 2002	Docket:	1565.006US1
Title:	METHODS, DATA STRUCTURES AND SYSTEMS TO REMOTELY VALIDATE A MESSAGE		

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

The applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request. This request is being filed with a Notice of Appeal. The review is requested for the reason(s) stated below:

REMARKS

This responds to the Final Office Action mailed on October 24, 2006. Claims 1-20 are presently in this application.

§103 Rejection of the Claims

Claims 1-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hruska et al. (U.S. 6,195,587) in view of Ranger et al. (U.S. 6,393,568). It is of course fundamental that in order to sustain an obviousness rejection that each and every element or step in the rejected claims must be taught or suggested in the proposed combination of references. Moreover, a proposed combination of references is not appropriate where there is no motivation from one of ordinary skill in the art to make such a combination in the first instance.

Applicants would further like to point out that the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art recited also suggests in some manner the desirability of the proposed combination. *In re Mills*, 916 F.2d 680, 16 USPQ 2d 1430 (Fed. Cir. 1990). Applicants would also like to note that “rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal

conclusion of obviousness. *See Lee*, 277 F.3d 1338, 1343-46 (Fed. Cir. 2002); *Rouffet*, 149 F.3d 1350, 1355-59 (Fed. Cir. 1998). This requirement is rooted in the Administrative Procedure Act, which ensures due process and non-arbitrary decision making, as it is in 35 U.S.C. § 103. *See id.*, at 1344-45.” *In re Kahn*, No. 04-1616 (Fed. Cir. March 22, 2006).

It has also been held that when the primary teachings of one reference is negated or taught against or taught away from another reference in the proposed combination, then it is common sense that one of ordinary skill in the art would not have been motivated to combine the references in the manner being proposed, because in so doing the very teachings that are asserted to be complimentary are by definition not complimentary to one another. Thus, there is no motivation by one of ordinary skill in the art to combine the references. It is also the case that the intended functions of the references being combined cannot be destroyed when combined. *See In re Grasselli*, 713 F.2d 731, 743; 218 USPQ 769, 779 (Fed. Cir. 1983).

Firstly, Applicants respectfully disagree that Hruska teaches receiving the email message in a first encrypted format. There is no indication at all that email is received in an encrypted format within Hruska. The only reference whatsoever to encryption is that a workstation, recipient or one consuming data, copies data to a file server for processing. This does not imply that an email was received at the workstation in encrypted format. It implies only that the workstation produces an encrypted format and then sends it to the file server for processing.

Secondly, Applicants respectfully disagree that Hruska teaches transferring, for the recipient, the decrypted email. Hruska is unambiguous as to how an item of data is processed from the workstation (recipient) to a file server (remote server). This is specifically called out in lines 41-67 of column 5. It is clear and unambiguous from reading these two paragraphs that the item of data to be processed is never received in a decrypted format by the file server (remote server). This is in fact precisely how it is done in Ranger as well and as was elaborated upon by the Applicants in the Response to the First Office Action. Specifically, in Hruska, the first method states that the workstation (recipient) “copies the file to be tested (in an encrypted form) . . . to the file server . . .” Hruska, col. 5, lines 44-45.

Clearly, this is not a teaching of transferring “decrypted email message contents to a remote server” because the Hruska teaching specifically calls for the file to be encrypted. The other method in Hruska begins on line 60 of column 5 and states “[t]he file to be tested is copied

to the file server as described above but instead of the file server scanning periodically for files to be tested, the transmitting workstation sends a packet message to the file server informing it that it has sent a file to be tested.” Hruska, col. 5, lines 61-67. This second method specifically states that it copies the file in the same manner as method 1 and method 1 copied the file in an encrypted format.

Therefore, Hruska specifically teaches against what Applicants have positively claimed in that a recipient sends a remote server email message contents that are decrypted; whereas both Hruska and Ranger specifically require that the file server or firewall server (Ranger) receive data in an encrypted format.

The Examiner cited all of column 5 for the purported teachings there is nothing even remotely present in this column to suggest that the file server receives a file in a decrypted format from the workstation as the Examiner proposes. In fact, the exact opposite is true from this column and from the entire teaching of Hruska. Therefore, Applicants respectfully disagree that Hruska can be used in support of teaching this particular limitation as recited in Applicants’ independent claims.

Moreover, Applicants have already demonstrated in the prior Response that Ranger cannot be used for this teaching and the Examiner appears to have acknowledged that fact by withdrawing the prior Ranger rejection for these teachings and now reciting Hruska for this teaching. But, Hruska teaches the opposite and the same as Ranger in this regard. Thus, the rejections cannot be sustained.

The Examiner further appears to acknowledge that the recipient or workstation of Hruska does not teach decrypting the file and relies on Ranger for decrypting. But, Applicants are respectfully confused. The limitation in the claim is not just for “decrypting” it is for providing in one manner or another a remote server with decrypted email message contents to process. Just reciting Ranger for a teaching of decryption takes the teaching of the Applicants’ claim limitations entirely out of context. That is, the remote server receives and processes decrypted contents and the client decrypts email message contents before supplying a decrypted version to the remote server. Applicants fail to see how adding Ranger to support just “decryption” somehow miraculously provides the full teaching enumerated above; namely the remote server processes decrypted email message content. In fact, this cannot be done with the proposed

combination because both Ranger and Hruska specifically require that the fire wall server or file server (remote server) receive and process files or data in an encrypted format. Thus, Applicants believe the proposed combination is still missing limitations and just because decryption is taught in Ranger does nothing to supply the missing limitations.

Therefore, Applicants assert that the Hruska lacks the teachings the Examiner appears to have relied upon and the Ranger reference fails to provide all the teachings needed to read on the limitations of Applicants' independent claims. Therefore, the rejections are not sustainable and should be withdrawn.

Finally, Ranger relies on communicating information via messages to the recipient that a file is good to view or not to view. Conversely, Hruska relies on using a signature of the file server via a checksum value associated with the file. Moreover, in Ranger both the recipient and the fire wall server rely on keys that are mutually known and communicated to decrypt the data and both work off of encrypted data. Thus, the two approaches are entirely different and it is therefore unlikely that one of ordinary skill in the art would have been motivated to combine the two. This is so because in Ranger there is no modification to the data being inspected by the fire wall server whereas in Hruska there is modification via the association of the checksum value. Hruska relies on the checksum as a primary teaching and to remove it would defeat the very purposes of Hruska. Conversely, Ranger relies on key exchange and removing it would defeat its purposes. The two approaches are different and not complimentary one uses a checksum and one exchanges keys. Thus, Applicants respectfully assert that not only does the proposed combination lack each and every teaching in the independent claims but the proposed combination cannot be made in the first instance.

CONCLUSION

Applicants respectfully submit that all of the pending claims are in condition for allowance, and such action is earnestly solicited. The Examiner is invited to telephone the below-signed attorney at (513) 942-0224 to discuss any questions which may remain with respect to the present application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

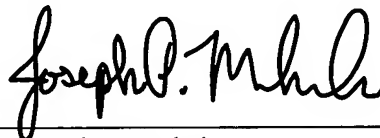
A. KENT SIEVERS ET AL.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(513) 942-0224

Date December 28, 2006

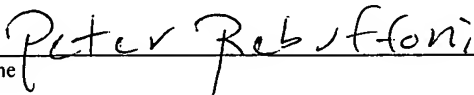
By /



Joseph P Mehrle
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 28 day of December 2006.

Name



Signature

